AU/AFF/NNN/2009-04

AIR FORCE FELLOWS

AIR UNIVERSITY

EQUIPPING NETWORK WARFARE:

INDUSTRIAL-ERA BUREAUCRACIES FOR

INFORMATION-ERA WEAPONS

by

Kevin D. Dixon, Lt Col, USAF

A Research Report Submitted to ESS/FO
In Partial Fulfillment of the Graduation Requirements

Advisor:
Dr. George Stein
Air War College

Maxwell Air Force Base, Alabama

April 2009

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **APR 2009**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**
4. TITLE AND SUBTITLE **Equipping Network Warfare: Industrial-Era Bureaucracies for Information-Era Weapons**		5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Command And Staff College Air University Air Force Fellows Maxwell Air Force Base, Alabama**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release, distribution unlimited**		
13. SUPPLEMENTARY NOTES		

14. ABSTRACT

Over the last decade, cyberspace proponents within the Air Force have articulated their mission areas vision, developed warfighting doctrine, and organized units at the wing-level and below for network warfare operations. Airmen have been trained, forces for network warfare operations have been fielded, and professionalization programs have been proposed. Additionally, senior leadership has made final decisions regarding the organization of Air Force cyberspace capabilities within a numbered air force and the presentation of those forces to the joint warfighting community through a major command. The Air Force has clearly moved forward in achieving its recently modified mission statement to fly and fight in cyberspace. It has satisfied key components of the DOTMLFP construct (doctrine, organization, training, materiel, leadership, facilities and personnel) necessary to field and sustain a mission area and its component warfighting capabilities. Based on the levels of development and investment in complementary mission areas, it can be presumed that similar efforts must have been made and advances realized in fielding materiel capabilities for cyberspace. It can also be presumed that these capabilities were largely developed within the framework of existing Department of Defense and Service-specific processes to develop more traditional warfighting systems, although perhaps compartmentalized. These corporate processes have been broadly criticized for their growing inability to provide traditional warfighting capabilities on schedule and within budget, while also satisfying threshold operational requirements. These delivery delays, cost overruns and requirement shortfalls occur 8 in the development programs of each Service, in programs developed for each operational medium (air, space, ground and maritime), and are independent of the prime defense contractor or magnitude of program investment. This suggests ingrained challenges underlying corporate processes and bureaucratic oversight means, as well as the organizational culture. One can anticipate that similar cost, schedule and requirements satisfaction issues would arise in network warfare programs employing the same mechanisms for traditional weapon systems procurement. However, the adverse consequences of the current corporate processes would be amplified if they were fully applied to cyberspace acquisition programs. The nature of network warfare operations and the more rapid technology change within the cyberspace domain places an increasing value on rapid capability delivery. Developed capabilities may have a limited lifespan of operational effectiveness, perhaps on the order of days, weeks and months; therefore, any process delay in providing cyberspace capabilities may make the delivered system obsolete by its delivery. Applying traditional requirements, resource and acquisition processes to the development of network warfare capabilities will ensure the Air Force has less-than-capable systems. This paper reviews the sufficiency of current corporate processes to field network warfare capabilities, and how those processes may prove incompatible with the nature of cyberspace conflict and its technological domain. Through interviews with senior policy makers, operational commanders, resource functional managers, acquisition professionals and private sector innovators, the author identifies obstacles to rapidly fielding network warfare capabilities within current Department of Defense corporate processes. Additionally, the author identifies potential solutions to these challenges by identifying suggestions and recommendations made by those interviewed.

15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**59**	

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Acknowledgements

This paper is based on information gleaned from first-person interviews. I sincerely appreciate the time, interest and pointed discussed offered by those helping me understand the complexities and differing perspectives associated with fielding network warfare capabilities. While document research and lessons learned reviews played a necessary and vital role in my research, these one-on-one interviews provided the most valuable insights to the challenges and potential solutions to rapidly fielding weapons for conflict in the cyberspace domain.

Those interviewed represent both past and current leaders in their area, whether senior decision makers, operational commanders, resource functional managers, acquisition professionals or private sector innovators. Without their willingness to share their perspectives, experiences, and recommended ways ahead, this paper would not have been possible.

I am particularly indebted to Dr. William Perry, former Secretary of Defense; Mr. R. James Woolsey, former Director of Central Intelligence; Dr. Sidney Drell, former member of the President's Foreign Intelligence Advisory Board; Colonel Bradford Shwedo, Commander, 67th Network Warfare Wing; and Mr. Robert Giesler, Vice President for Cyber Programs, Science Applications International Corporation. Their counsel, frank discussion and seasoned commentary on the challenges facing network warfare operations were invaluable.

Additionally, I wish to thank those cyberspace community leaders and subject matter experts who offered their valuable time in orienting my research and highlighting their perspectives, as well as those of their assigned organizations. Without fail, they addressed my requests for information in detail and challenged me to think beyond my initial research framework.

I pass my sincere thanks to Mr. Phillip Taubman, New York Times Assistant Editor and Consulting Professor, Freeman Spogli Institute; Mr. Robert Lundy, Chief Executive Officer, GlimmerGlass Corporation; Mr. Randy Brown, SES, Deputy Director of Intelligence and Requirements, Headquarters Air Force Materiel Command; Dr. John Bay, Chief Scientist, Air Force Research Lab Information Directorate; Dr. John Parker, Chief Technical Officer, GlimmerGlass Corportation; Mr. J. Michael Kretzer, SES, Technical Director, Air Force Information Operations Center; Mr. Chusak Siripocanont, Vice President of Engineering and Operations, GlimmerGlass Corporation; Lt Col Fred Baier, Information Operations Program Element Monitor, Office of the Secretary of the Air Force; Lt Col Shane Ducommen, Chief, Offensive Information Operations, Headquarters Air Force; Lt Col James Lance, Deputy Commander, Air Force Network Operations Center; Lt Col Debra Zides; Chief, Cyber Warfare Integration Office, Air Force Materiel Command; Lt Col Tamara Schwartz, Chief, Capabilities Integration Office, Air Force Materiel Command; Lt Col Douglas Coppinger, Commander, 91st Network Warfare Squadron; Capt Eric Stride, Cyber Operations Action Officer, 67th Network Warfare Wing; Mr. Jeffrey Faucheux, Advanced Programs Manager, Harris Corporation; Mr. Michael Minter, Defense Contractor, MITRE; and Mr. John Clemens, Defense Contractor, Northrop Grumman Corporation.

Every attempt has been made to accurately capture the context and intent behind the comments made during these interviews. Any misrepresentation or misquote is solely my unintentional error. No classified information regarding network warfare was referenced, requested or addressed during these interviews. In fact, specific efforts were made to emphasize unclassified process and oversight mechanisms to avoid any potential dialogue regarding current or planned capabilities. Any suggestions regarding network warfare plans, programs, capabilities or limitations are based solely on my assumptions and conjecture.

Finally, I wish to thank the leadership, overseers and fellows of the Hoover Institution for War, Revolution and Peace, located at Stanford University. They have provided a superb research environment and offered a broad palette of learning opportunities to the National Security Affairs Fellows. This fellowship provided frequent opportunities to explore complementary or indirectly-related issues associated with my research. I thank Dr. David Brady and Ms. Joy Kelley for making this an incredibly memorable and rewarding professional experience.

Abstract

Over the last decade, cyberspace proponents within the Air Force have articulated their mission area's vision, developed warfighting doctrine, and organized units at the wing-level and below for network warfare operations. Airmen have been trained, forces for network warfare operations have been fielded, and professionalization programs have been proposed. Additionally, senior leadership has made final decisions regarding the organization of Air Force cyberspace capabilities within a numbered air force and the presentation of those forces to the joint warfighting community through a major command.

The Air Force has clearly moved forward in achieving its recently modified mission statement to fly and fight in cyberspace. It has satisfied key components of the DOTMLFP construct (doctrine, organization, training, materiel, leadership, facilities and personnel) necessary to field and sustain a mission area and its component warfighting capabilities. Based on the levels of development and investment in complementary mission areas, it can be presumed that similar efforts must have been made and advances realized in fielding materiel capabilities for cyberspace. It can also be presumed that these capabilities were largely developed within the framework of existing Department of Defense and Service-specific processes to develop more traditional warfighting systems, although perhaps compartmentalized.

These corporate processes have been broadly criticized for their growing inability to provide traditional warfighting capabilities on schedule and within budget, while also satisfying threshold operational requirements. These delivery delays, cost overruns and requirement shortfalls occur

in the development programs of each Service, in programs developed for each operational medium (air, space, ground and maritime), and are independent of the prime defense contractor or magnitude of program investment. This suggests ingrained challenges underlying corporate processes and bureaucratic oversight means, as well as the organizational culture.

One can anticipate that similar cost, schedule and requirements satisfaction issues would arise in network warfare programs employing the same mechanisms for traditional weapon systems procurement. However, the adverse consequences of the current corporate processes would be amplified if they were fully applied to cyberspace acquisition programs.

The nature of network warfare operations and the more rapid technology change within the cyberspace domain places an increasing value on rapid capability delivery. Developed capabilities may have a limited lifespan of operational effectiveness, perhaps on the order of days, weeks and months; therefore, any process delay in providing cyberspace capabilities may make the delivered system obsolete by its delivery. Applying traditional requirements, resource and acquisition processes to the development of network warfare capabilities will ensure the Air Force has less-than-capable systems.

This paper reviews the sufficiency of current corporate processes to field network warfare capabilities, and how those processes may prove incompatible with the nature of cyberspace conflict and its technological domain. Through interviews with senior policy makers, operational commanders, resource functional managers, acquisition professionals and private sector innovators, the author identifies obstacles to rapidly fielding network warfare capabilities within current Department of Defense corporate processes. Additionally, the author identifies potential solutions to these challenges by identifying suggestions and recommendations made by those interviewed.

Chapter 1

The Cyberspace Domain

> *As weapons increase in lethality, precision and standoff, intercepting any hostile platform early in its flight is increasingly important.*
>
> — General Ronald R. Fogleman, 16th Chief of Staff, United States Air Force

When the Air Force added cyberspace to its mission statement in 2005, it defined a new domain for Service operations.[1] The cyber domain joined those of air and space, the traditional Air Force operating environments. The Air Force has now established plans to form a cyberspace-focused, 24th Air Force within Air Force Space Command, and is developing its network warfare capabilities to enable joint operations.[2]

Additionally, the Air Force has established a functional management office within the Air Staff, has created a formal schoolhouse and force training pipeline, and is designating a new Air Force specialty code for the information operations career field.[3] In developing a viable warfighting capability, the Air Force is clearly investing resources towards the organization and training of cyberspace forces.

[1] Air Force Link, "Air Force Releases New Mission Statement," http://www.af.mil/news/story.asp?id=123013440 (accessed 10 December 2008).

[2] Headquarters United States Air Force Program Action Directive 07-08, "Phase I of the Implementation of the Secretary of the Air Force Direction to Organize Air Force Cyberspace Forces," 20 February 2009.

[3] Air Force Cyber Command, "New Cyberspace Career Fields, Training Paths, Badge Proposed," http://www.afcyber.af.mil/news/story.asp?id=123104963 (accessed 15 Dec 2008).

As aerospace capabilities were developed previously and then further advanced over time, the new cyberspace community will similarly work towards defining its warfighting potential and desired mission capabilities. It will satisfy these mission area objectives through the DOTMLFP (doctrine, organization, training, materiel, leadership, facilities and personnel) construct. Just as the other aerospace operations and capabilities evolved through this process, so too will those within the cyberspace arena. It should be expected that a military leadership culture would apply well known and previously applied techniques to a new challenge, particularly one as daunting as establishing a new warfighting domain for its Service.

Cyberspace operations, although new and developing in its operational concepts, does share common elements with air and space operations, namely global reach and global strike. Similarly, cyberspace operations would strive to achieve combat advantage over adversaries through effects-based objectives, stealthy approach and precision engagement. Senior decision makers within the Department of the Air Force have made use of these commonalities in helping develop, shape and communicate their vision for future cyberspace operations.

It is understandable that they do so, as it enables Airmen to map their understanding of other known elements of aerospace capabilities to the new and lesser known realm of cyberspace operations. Even such challenges as force organization and presentation of cyber-focused forces can be made less daunting by relying on the experiences and lessons learned from the Air Force's more traditional air and space missions.

The cyberspace domain and the network warfare operations conducted within it, however, may prove to be so unique that past leadership approaches, processes and mindsets might not be so easily applied. Particularly in the area of materiel development, the operational requirements of network warfare systems may be so different that the broad application of current processes may actually hinder the rapid delivery of relevant capabilities. Applying what may be recognized as tried and tested resource management processes to the development of cyberspace systems might lead to operational shortfalls.

Clearly, there are benefits in following known methods in organizing the cyberspace mission and its capabilities; however, the cyber domain is sufficiently different from more physical-based domains to suggest there are limits to imposing traditional business practices on it. The defining characteristics of cyberspace, its operating environment and its technology-enabled capabilities are such that the inefficiencies of traditional corporate management actions are amplified when applied to the cyber domain. The unintended consequences of such broad process templating may very well prevent cyberspace forces from fulfilling the Air Force's vision for their future operational effectiveness.

The examination of these corporate processes and their unintended effects on network warfare systems development will be reviewed in this paper, as well as consideration of potential alternatives as proposed by senior leaders and subject matter experts within the cyberspace community. Before the potential problems can be identified and alternatives proposed, however, a quick orientation to the cyberspace domain and network warfare operations is necessary. Its doctrinal components, mission area objectives, potential mission sets and network warfare systems must be mentioned, with particular consideration of the technological influence on its potential success.

Network Warfare Doctrine

Although there are slight differences in terminology, joint and Air Force doctrine agree in concept regarding the nature and components of network warfare. The joint doctrinal publication defines these as:

> Computer Network Operations: comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.
>
> Computer Network Attack: actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
>
> Computer Network Defense: actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks.
>
> Computer Network Exploitation: enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.[4]

Likewise, network warfare operations are defined in Air Force doctrine as:

> Network warfare operations: integration of the military capabilities of network attack, network defense, and network warfare support.
>
> Network attack: employment of network-based capabilities to destroy, disrupt, corrupt, or usurp information resident in or transiting through networks.
>
> Network defense: employment of network-based capabilities to defend friendly information resident in or transiting through networks against adversary efforts to destroy, disrupt, corrupt, or usurp it.
>
> Network warfare support: collection and production of network related data for immediate decisions involving network warfare operations. [5]

[4] Joint Staff. *Joint Publication 3-13: Information Operations.* Washington D.C.: Joint Publication, 13 February 2006.

[5] Air Force Doctrine Center. *Air Force Doctrine Document 2-5: Information Operations.* Maxwell AFB, AL: Air Force Publications, 11 January 2005.

In reading these doctrinal definitions, technological terms are used frequently to describe the operating environment, the nature of "on-net" operations, and the elements to be targeted, defended and exploited. Whether the terminology used is network, computers, data or systems, the underlying theme is technology. It is man-made technology that defines the medium in which cyberspace operations occur.

In contrast, other domains of military conflict are defined by the physical arena in which the operations take place. The nature of air, ground, maritime and space operations may incrementally change as new materiel, tactics and training are introduced. Similarly, technological advances and innovation may enable new operational advantages in traditional warfighting domains. The underlying characteristics of those domains are unchanging, however. Geography and physics define and constrain air, ground, maritime and space operations, not technology.

"In no other area is the pace and extent of technological change as great as in the realm of information," said the Air Force's strategic vision document, "Global Engagement: A Vision of 21st Century Air Force."[6] Written in the 1990s following the early concept development of command and control warfare and then information warfare, this statement is still accurate today. If network warfare operations are focused on technology-intensive systems such as computers, networks and automated information systems, then one must consider how network warfare systems will maintain technological pace as changes occur within those targeted systems. Effective cyberspace operations will be largely determined by our ability to remain within technological reach of the networks we wish to target.

[6] HQ USAF/XP, "Global Engagement: A Vision for the 21st Century," http://www.au.af.mil/au/awc/awcgate/global/competencies/information.htm (accessed 15 January 2009).

Mission Area Objectives

Network warfare operations have the ultimate objective of satisfying or enabling the operational commander's warfighting intent across the spectrum of potential combat operations. Those objectives might be achieved in a kinetic combat engagement, or they may be purposeful operations to shape an adversary's battlespace awareness. How cyberspace forces and systems will contribute to operational success is somewhat dependent upon the tasks assigned to them.

An operational commander will consider available combat systems and tactics to best achieve his objective within imposed constraints, whether those be based on political, geographic, resource, time or rules of engagement limitations. His courses of action may leverage lethal and non-lethal options, while also exploiting firepower and maneuver advantages. Although their applicability will differ in every military scenario, network warfare operations are intended to either enable other elements of combat power or serve as the primary means to affect the adversary, while also protecting friendly force networks and their information.

Network warfare operations are no different from the more traditional combat arms in seeking to manipulate adversary behavior. Military operations in all domains seek to influence the adversary, ultimately with the intent of forcing the adversary to yield to our desired outcome; however, only operations within cyberspace do this solely by seeking to affect information and the systems on which that information is passed.

Focusing on the attack element of network warfare operations, cyberspace forces would employ materiel capabilities to deny, degrade, deceive, disrupt, destroy or otherwise neutralize the targeted adversary information components. Those targeted elements may be hardware, software or information-based in nature, and the immediate objective may be to affect a specific network, a defined data set or perhaps a secondary system either controlled or influenced by the initially targeted system. Intelligence-oriented operations would likewise seek to extract and exploit information resident on the adversary's systems or moving within their networks. And defensive operations would seek to ensure protection from such attacks conducted by the adversary.

It must be noted that other warfighting elements, such as electronic warfare and psychological operations, have the ability of attacking the adversary through non-kinetic means. However, an important distinction arises when noting that network warfare is the only non-kinetic means to affect the adversary at the information-level. That is to say, network warfare systems have the potential to maneuver on the adversary's network to dynamically shape his orientation and affect future actions.

The desired effect of these network operations is to shape the adversary's orientation to the battlespace and our operations, as well as his future actions. The methods are through the destruction of data, manipulation of networks or deception of enemy combatants. The manner in which these operations will be executed may vary with the type of system targeted or the nature of the information within the network.

Combat operations within other warfighting domains also seek to gain advantage over the adversary, with the objective of gaining supremacy or dominance over the adversary. Just as Airmen seek to gain air dominance over hostile air forces, Airman conducting network warfare operations also seek to gain advantage.

Information superiority enables our forces to better understand events within the battlespace at both a qualitative and quantitative advantage, enabling leadership to more quickly exploit opportunities and recognize vulnerabilities. This information advantage enables a more defined knowledge regarding adversary capabilities and actions, while concurrently attempting to minimize the adversary's understanding of friendly forces. So important is the concept of information superiority, it is included as one of the Air Force's six core competencies.

As is the case with technological infrastructure, the pace is rapid in the fielding of new information-based applications. The initial appearance of an application may be followed within months by a more capable model by the same manufacturer or an entirely new offering may be available from a different vendor having a different proprietary concept. Each version of the application may have different performance characteristics and be protected by different security protocols, each with differing levels of maturity.

Network warfare operations have already been characterized by the need to affect technology-intensive systems, with particular consideration given towards the pace in which technology may change within the targeted network. Now one must also consider how quickly applications and security occur within the network. Effective network warfare systems must be able to adapt quickly to the changing environment which they are being tasked to affect.

Potential Target Sets

Both Department of Defense and Air Force doctrine documents identify networks, computers and resident information as potential targets of network warfare operations. That these technological elements might be the focus of an attack or exploitation, as well as being protected in defense, is clear. As discussed previously, keeping pace with the enabling technologies and information applications will be one challenge to effective cyberspace operations. However, this rate of change is not constant across the adversaries we might face in conflict. Additionally, there are varying degrees of sophistication in the information networks of potential adversaries. One must consider how cyberspace capabilities will be developed that will have the breadth of utility and depth of capability to achieve their desired effects.

A near-peer competitor with a sophisticated telecommunications network and developed infrastructure suggests that this might be more challenging target. Certainly the scope of potential network targets would be large, as would be the associated information applications and data. But what of the challenge posed by a non-state actor involved in a transnational threat towards our interests?

A non-state actor such as a terrorist group is not obligated to establish a traditional telecommunications network to coordinate its activities. Instead, it may exploit the telecommunications infrastructure of its unwitting host country, employing civilian networks, personal communications devices and commercially available applications to coordinate its actions. This suggests that network warfare capabilities will have requirements to affect networks, computers and information on both government and commercial networks. This increases the level of sophistication required for attack and exploitation, as well the breadth of systems against which cyberspace operations may be directed.

Further, it points towards the need to keep pace with technology development efforts in both government and commercially-fielded systems. In decades past and prior to the transformation of analog-to-digital communications, government interests and large corporate investments produced the grid on which information was transferred and provided the information systems in which data was used. Innovators and small start-up companies can now provide new alternatives to networks, computers and information applications, often bundling them with other capabilities for unanticipated uses.

This indicates that future cyberspace capabilities will not only have to consider commercial networks, but also the pace in which new technology enters the market place. In the example of the non-state actor, he may continually adopt the latest commercially available systems, applications and encryption to coordinate his group's efforts, posing a moving target in the cyberspace domain and becoming increasingly more difficult to affect. Not only will cyberspace operations require maneuverability on both government and commercial networks, but they must also consider the potential of pop-up technological challenges posed by commercially-available systems and applications.

The methods and means to a successful network attack or exploitation must also consider the purpose and sophistication of the targeted network. Military networks and senior-level nodes may prove the most difficult, with varying levels of security and encryption. But what of civilian networks on which targeted systems may operate? Is the operational commander's intent to disrupt the electric grid or transportation network? Perhaps he wishes to affect only certain regions of the battlespace while omitting others from the attack. How might network operations be conducted against a hardened or deeply buried target?

The intent here is not to show how difficult network warfare might be, but rather to emphasize the breadth of targets and different networks which cyberspace forces might be directed to affect. Certainly there is a limit to network warfare's operational reach; however, the above situations could all be worthwhile operational requirements of a network warfare platform. This suggests that the breadth and unique nature of the potential operational tasks will require some level of adaptable systems to target new and emergent targets, as required by the operational commander.

Network Warfare Systems

The Air Force efforts to establish command and control structures, as well as identify force development needs, provide the framework for the Service's future network warfare potential; however, it is the procurement and employment of operationally-relevant materiel capabilities which will provide the substance of the mission area's warfighting utility. As the Air Force implements its plans to establish a cyberspace mission area, it must also invest resources to develop, acquire and field cyberspace capabilities. These network warfare systems will enable defensive, offensive and intelligence-gathering missions within the cyber domain.[7]

Network warfare systems, comprising both hardware and software elements, will form the materiel component of these cyberspace-domain capabilities. These are not new concepts to military weapon systems development. Technology-intensive components have been integrated into traditional weapon systems for decades. However, the hardware and software requirements of cyberspace weapons platforms will be unique, driven by the defining characteristics of their domain and most notably by the pace of technology advances in the targeted network.

There does not appear to be a standard template for how a network warfare system will look, operate or be employed. A system will be tailored to its specific cyberspace mission, whether offensive, defensive or intelligence-focused. For those developed for network attack, a critical attribute may be stealthy electronic access to a single targeted network. Defensive systems, in comparison, may require broader integration into a multi-layered, joint or coalition network security structure. Intelligence-oriented network warfare efforts may rely on human emplacement of devices to gather and extract information from a single targeted computer.

[7] Joint Staff. *Joint Publication 3-13: Information Operations.* Washington D.C.: Joint Publication, 13 February 2006.

Clearly, the mission purpose will drive the form, fit and function of the component cyberspace systems. There could not be a single system which performs all network warfare operations or a single system to execute all missions within one area. This indicates that multiple platforms may exist, each tailored for its specific mission and target.

The opportunities presented by network warfare operations are balanced by its challenges. Robust sensor suites for defensive operations, stealthy access mechanisms and tools for network exploitation, and the precision employment requirements of offensive capabilities must maintain their effectiveness in a medium defined by frequent, swift and steady technological advances, as well as innovative applications of that technology. Whereas the mediums of air, space, maritime and ground conflict are constrained by unchanging physical characteristics, the cyberspace medium is continually evolving based on how technologies and innovations are applied.

This suggests that the hardware and software components of network warfare operations will be continually evolving to maintain or secure freedom of action in the cyberspace domain. Defensive sensors and software packages will be continually updated to address new and emerging threats. Intelligence gathering methods and applications will be ever evolving to exploit both technological opportunities and adversary weaknesses. Offensive capabilities will demand constant modification to ensure they can achieve their desired effects against adversary networks and applications in constant flux.

Chapter 2

The Challenges

Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur.

Giulio Douhet, Italian general and early air power theorist

If cyberspace operations are to be successful, it will be due to its trained personnel, developed tactics, techniques and procedures, and capable suite of network warfare systems. It is the development of these materiel capabilities which may well prove the most difficult task, as noted previously in the discussion of doctrine, mission area objectives, potential target sets and the nature of network warfare systems themselves. The breadth of targets, differing nature of potential adversaries, varying degrees of network sophistication and need for frequent system adaptation will all be difficult to overcome in their own regard.

The development of materiel solutions to address these operational obstacles will be particularly difficult. In the best of circumstances, maintaining technological reach of all objective target sets would be a resource-intensive effort. Compounding this are additional challenges in the requirements, resource and acquisition processes which will amplify the magnitude of an already difficult objective. These are the breadth of technological change, the pace of technological innovation and the operators' demands for rapid capability delivery.

Breadth of Technological Change

Network warfare operators will be tasked to not only defend their networks, but attack and enable the exploitation of adversary systems. These networks, both friendly and adversary, are defined by the systems, links and applications which are employed on them. Clearly, these are technology-intensive targets and it can be assumed that an equally advanced technological system would be required to sufficiently defend, attack or exploit it.

A key challenge to future network warfare operators will be in maintaining their ability to affect a targeted network as that system is upgraded and transformed over time. Previously designed systems to provide access and affect the network may become ineffective should those vulnerable areas be modified. To appreciate the breadth of technological change and its potential impact on offensive cyberspace operations, it helps to consider a representative network that might be the target of a network warfare operation.

In general, networks can be described as a system of systems, with multiple levels of component hardware and software within each. A cellular communications network, for example, will consist of mobile handsets. They will communicate to a fixed base station while within its radio line of site and then these handsets will be transferred to the next nearest base station within the network. Communications between the mobile caller and the call recipient will be routed through the base station and then through some medium, either fiber, cable or via radio frequency, to a central switching office. In turn, the call will be routed back to another base station within the same network or it will be distributed through a public switching network to the intended recipient.

This description of personal communication systems through a mobile network, although oversimplified, is complex enough and one can appreciate the technological challenges associated with either infiltrating or attacking such a network. However, the description above pales in comparison to the technical details omitted. No mention has been made of potential differences in the numerous mobile phone devices available or the encrypted nature of the communication. Nor has there been discussion of the complex billing and routing software used to identify mobile subscribers with access privileges to that individual mobile network, or the antenna arrays used to receive and transmit data to the mobile communications device. Additionally, no mention is made of the content of the digital data stream, whether that be audio, still or moving imagery, or data for other purposes.

The scope of the potential challenges associated with technological change can be seen when considering any individual component of the network. The mobile handset itself may have a certain type of security or processor that exceeds that of its predecessors. The encrypted communications between the personal communications device and the base station tower might be modified over time, as might be a different set of security protocols applied to the communications links between the base station and the central switching station. Software might be upgraded throughout the system, ranging from the handset to the underlying call set up software to the supporting network software

An offensive or intelligence-focused, network warfare effort may have had some level of initial success in accessing the network when it was in a certain technical configuration. But can the same level of access can be assured when those configurations are changed? Upgrades and changes can occur on a frequent basis, with no advance indication of the pending modification. The potential effect on cyberspace operators might be that they now cannot penetrate the targeted network to achieve their desired effects. The breadth of technological change, then, is a consideration that must be made when determining how network warfare systems will be developed and the processes used to guide that development.

Pace of Technological Innovation

The consequences of widespread configuration changes pose daunting challenges themselves. Compounding the scenario and making it an even more difficult obstacle is the pace at which these changes may occur. A dedicated effort to maintain illicit access to a single network might be possible as an individual component is modified, but how well might that capability perform when multiple components on the targeted network are being upgraded and on a frequent basis? The pace of technological innovation may pose the most serious challenge to network warfare operators, causing a never ending cycle of technological reconnaissance to determine the as-then current make up of the targeted network.

This pace of technological change may vary with the type of network. Government-managed or military-controlled networks may change at a slower pace, but the modifications themselves may be far more advanced than what might be seen in the commercial sector. Commercially operated systems might experience change at a much more constant rate, although some components within the network may be modified more frequently and at a magnitude beyond that of other elements. Hybrid systems, commercial systems that are being used for government or military purposes, suggest a third consideration. The end user of a hybrid system may drive performance or security requirements that can be achieved quickly due to the influx of government investment.

Users on a potentially targeted network will drive the operational requirements of the system; however, the technological leaders responsible for its development will identify the solution and opportunities for improved network performance. Network warfare operators will be somewhat reactive to these technologists and network administrators as they modify the systems which the cyberspace forces seek to attack.

Just as those responsible for our networks, adversaries are also going to consider modifications which improve performance, increase security and offer advanced capabilities. In-house design may lead to some improvements in the marketplace; however, it will largely be the commercial marketplace which provides the broader set of available options. With the past two decades as a guide, one can see how quickly new systems or more capable applications become available.

A term often used to describe this rapid pace of technological innovation, particularly with respect to the Internet, is the "web year."[8] [9] First described in the mid-1990s during the "dot com" boom, it describes the speed at which new developments occur in web-based applications. The web year is defined as that time period of discovery and innovation which roughly equals the technological evolution in other, more traditional development areas within one calendar year. There is no set time period which equates to a web year, but its proponents suggest periods as short as two months to perhaps as long as four months. What is clear is that there are multiple development cycles occurring within a single calendar year.

How might this pace of technological advancement affect network warfare operations? As described previously, the breadth of technological change is immense within the network.

[8] Search SOA, "Web Year," http://searchsoa.techtarget.com/sDefinition/0,,sid26_gci853845,00.html (accessed 15 December 2008).

[9] BX.com Terminology Reference, "Web Year," http://www.bx.com/dictionary/ecommerce/Web_year.cfm (accessed 15 December 2008).

Numerous components, both hardware and software, might be adapted for new capabilities. Compounding that might be the frequency of change. Using the most conservative of estimates of a web year equating to four months, then there is potential for three innovation cycles which might be applied to the network within a single year.

This is not to say that only materiel components would be affected by the pace of technological change. Advancements in individual components or certain segments of the network might be one consideration, but so would the unforeseen applications of that new technology. Not only does the web year refer to the development of components, but how those different technologies and applications might be bundled to present the user new capabilities. A single calendar year of development might see two or more unexpected applications which now might be adopted via “commercial off the shelf” processes by a potential adversary, providing a new pop-up application. Depending on how that application or device might be employed and its importance within the adversary network, it may require network warfare operators to develop a new capability to target or exploit it.

Operational Urgency Demand

Network warfare operators will face significant challenges in maintaining advantage against their targeted networks. As noted earlier, the breadth of systems and how those networks are employed by the adversary will make the technical challenges to achieving operational effects difficult. Adding to this may be the adversary’s unanticipated modifications to their network, either by upgrades or new applications, at a pace difficult for cyberspace forces to either keep abreast or forecast.

As in any other warfighting domain, development and operations within the cyberspace medium will occur in a resource constrained environment. There are only so many capable personnel and funds available, and a finite number of development efforts which might be undertaken. This places increasing importance on the requirements generation process, where senior leadership can focus the limited resources available on the highest priority items. In the area of cyberspace operations, these priorities will be guided by continual assessment of the most likely and most dangerous scenarios, as well high-payoff efforts which may address shortfalls and add capabilities in multiple areas.

With the nature of the cyberspace domain, these requirements may be generated by commanders and operators frequently. They might be identified through intelligence assessments of potential target networks or the realization that previously fielded network warfare tools are no longer effective against the designated systems. A more likely and dangerous scenario may be the emergent target set that pops up as part of a contingency operation or combat engagement.

Conventional military forces and their associated materiel may also experience these contingencies and engagements; however, their combat materiel may be largely operationally effective regardless of the location of the fight or the adversary. Geography, climate, operating environment and adversary capabilities will vary with every operation, and the deployment of conventional air, ground and maritime units will be tailored for the scenario. Given the current defense procurement processes, materiel capabilities supporting these units are intended to operate in a wide variety of environments and against a spectrum of potential adversaries and threats. Instead of rapid materiel adjustments to address the changing operating environments, conventional military forces modify their tactics or leverage other advantages against the adversary.

Network warfare systems, however, operate in a different medium of conflict. The challenges faced by cyberspace capabilities are defined by the very nature of the environment in which they operate. Variations of technology, adversary systems and how adversary forces employ those networks indicate an operating environment of a much different nature for cyberspace forces. These network warfare elements may find themselves being tasked to achieve effects in networks against which they had not anticipated or had not yet committed resources to develop capabilities. Effectively prevented from accessing or affecting the network, operators may not be able to modify their tactics as conventional military forces may do.

Once identified as potential networks of interest, operators will begin their target and technical analysis. Technical reconnaissance or other means may identify vulnerabilities or methods to affect the adversary system or the information within it. In turn, emergent requirements will be identified to exploit these newly found vulnerabilities in the hostile network. Techniques might be developed which leverage existing capabilities in new operating schemes, but it is just as likely that new technological developments must be initiated to satisfy the emergent requirements.

Battlespace leaders and conventional forces have long made use of the “OODA loop” to describe how they make decisions in combat. This concept describes how decision makers observe, orient, decide and act in complex and dynamic combat environment.[10] The objective of the combat leader is to compress the OODA loop so that he achieves awareness of the battlespace and adversary actions, while deciding his course of action and then implementing it

[10] Value Based Management, “Information Warfare OODA Loop,” http://www.valuebasedmanagement.net/methods_boyd_ooda_loop.html (accessed 20 January 2009).

before his adversary can do the same. Cyberspace operations will also employ this OODA loop concept; however, the outcome of the decision cycle may force some ways ahead that would be unlikely in conventional combat engagement.

When tasked with affecting a network in an unanticipated operating environment, the cyberspace leadership may observe that new technologies or applications have been implemented on the adversary's system. Similarly, they may orient to a preferred course of action that requires modification or a new development effort to specifically target a vulnerable node. This suggests that the OODA loop, as applied to the cyberspace domain, may orient its immediate actions towards technological development efforts to achieve operational effectiveness against these newly identified target networks.

The focused operational attention to a specific adversary, network, application or information-based target will likely generate operational requirements to the supporting resource and acquisitions community. This sense of operational urgency, both in breadth and volume, may overwhelm the enabling technologists which would be tasked to provide a materiel solution within a short delivery cycle. Challenging as that may be, the operational community and capability developers will also have to contend with corporate processes intended to oversee the development of materiel solutions for combat forces. The operational sense of urgency to acquire and field these emergent requirements may clash with the timeframe associated with the bureaucratic processes satisfying the need.

Chapter 3

Industrial-Era Corporate Processes

It's not technology. This is culture. This is the imperative to change, and be convinced that the imperative is real and will advantage us. Getting the inertia going to get the system changed is the challenge that's in front of us.

— General James Cartwright, Vice Chairman, Joint Chiefs of Staff

To gain or maintain operational advantage in network warfare operations, rapid capability development, acquisition and fielding must be the norm and not the exception for cyberspace platforms and tools. This is essential to enable operational capability against both emerging targets, changing networks and new technologies. However, current Department of Defense and Air Force processes do not support or enable this operational necessity. The current requirements generation process, resource allocation process, and traditional acquisitions methods do not effectively support network warfare operations.

The development, procurement and deployment needs within the cyberspace domain differ from more traditional military systems. These differences are brought about by the nature of the cyberspace medium, its enabling technology, and the rapidity in which technological advances may be generated. Unlike the traditional warfighting domains and their ability to affect their targets, cyberspace operations are much more dependent on and vulnerable to rapid changes in the technological landscape. Just as operators must change their tactics to a new threat or changing environment, so too must corporate processes be modified when they are unable to effectively support the operational requirements.

The current defense planning, programming and budgeting system traces its roots to 1961 and then-Secretary of Defense Robert McNamara. It was developed with the intent towards coordinating resource investment and capability development decisions across the Department of Defense. It was a necessary improvement given the nature of military systems procurement and development at the time, allowing the department to focus on an "output oriented, well documented, (and) systematically accountable" process.[11] While the planning, programming and budgeting processes have evolved over time, its emphasis remains focused on identifying and prioritizing operational capability needs and allocating limited resources to address those needs.

Requirements generation and system acquisition processes also found their start in the Cold War era. The Department of Defense sought to synchronize weapons development efforts with identified warfighting requirements, while also providing an oversight mechanism to oversee the programs which had been initiated. The requirements process linked Service visions and planning regarding future capabilities with those warfighting constructs and operational needs identified by the Department of Defense and joint warfighting commands. Similarly, acquisition directives and regulations provided a consistent business process for military acquisition efforts, the program offices which direct them and the defense contractors funded to build the capability.

These corporate processes have been frequently criticized on their ability to satisfy operational requirements, while remaining within cost and delivery schedule constraints. A 2008 report by the Government Accountability Office found that current acquisition programs were

[11] Carol L. DeCandido, *An Evolution of Department of Defense Planning, Programming and Budgeting System: From SECDEF McNamara to VCJCS Owens*, US Army War College Strategy Research Project (US Army War College, Carlisle Barracks, PA, 4 June 1996).

delayed on average over 21 months in "delivering initial capabilities to the warfighter."[12] And despite past efforts to improve corporate processes within the Department of Defense, it appears as if they've not had positive effect. This delay represents a five-month increase over the Government Accountability Office's assessment of systems delivered in Fiscal Year 2000.

Not only have capability delivery times increased, so too have the costs. The same report found that overall research and development costs exceeded their budget by 40% in Fiscal Year 2005 (up from 27% in 2000), while total acquisition costs were over initial cost estimates by 26% in Fiscal Year 2005 (up from 6% in 2000).[13] Worse still, the "programs (the Government Accountability Office) assessed failed to deliver the capabilities when promised" and more than 14% of acquisition programs were more than four years late in providing a capability.[14]

Similar statistics for how cyberspace programs perform in development and acquisition processes are not available; however, it is useful to consider other technology-intensive efforts as a close approximation. The Vice Chairman of the Joint Chiefs of Staff, General James Cartwright, recently commented that "the current method of procurement for information technology is so slow that by the time software systems and the like are purchased, they're out of date."[15] His comments were amplified further by Mr. Robert Carey, the Navy's chief information officer. "The acquisition system is a challenge. Things are moving really fast," said Mr. Carey. "The acquisition system and more importantly, the budgeting system, move at a different pace."[16]

[12] US Government Accountability Office, *Defense Acquisitions: Fundamental Changes are Needed to Improve Weapon Program Outcomes,* Testimony before the US Senate, GAO-08-1159T (Washington DC, 25 September 2008), 2.
[13] Ibid, 4.
[14] Ibid, 2.
[15] Antonie Boessenkool, "DoD IT Procurement Too Slow: Cartwright," Defense News, 4 March 2009.
[16] Ibid.

Based on interviews with senior leaders within the Air Force network warfare community, there appears to be similar concern with the current corporate processes and their suitability for equipping cyberspace forces. Colonel Bradford Shwedo, commander of the 67th Network Warfare Wing, commented that development needs and operational demands of cyberspace systems "do not lend themselves to being satisfied" by current Department of Defense and Air Force processes to field more conventional weapon systems.[17] Instead of making adjustments within these processes, he finds those responsible with satisfying the stated operational requirements are "retreating to what's comfortable for them."[18]

Our current corporate processes were developed in a different time and faced different challenges. Certainly there is a need for oversight, prioritization schemes and the close linkage of investments with the most important materiel development and procurement efforts. Cyberspace systems, however, may prove more difficult to develop within these established processes. Through interviews with those closely associated with these processes, one is led to believe that changes should be made and allowances considered for the unique aspects in equipping network warfare forces.

Requirements Generation Process

Multiple inputs drive requirements generation to some degree, each providing their own level of direction and fidelity to future weapons systems. The Service's vision and the functional area's Mission Area Plan provide the conceptual framework of the mission area's contribution to warfighting, as well as a macro-level identification of gross mission capabilities. These documents do not provide sufficient detail to drive a specific weapon system's development, but

[17] Col Bradford Shwedeo (67th Network Warfare Wing), interview by the author, 25 February 2009.
[18] Ibid.

they do indicate Service and major command-level advocacy for systems that may satisfy the Service's vision and mission area planning needs.

Mission Needs Statements from either joint combatant commands or Air Force major commands are the first documents that provide a more refined level of detail to the both the functional area or acquisitions community that an operational need exists which is not being satisfied by a current capability or development effort. A more pressing operational deficiency is identified through a Combat Mission Needs Statement or Joint Urgent Operational Need statement. These receive the highest visibility due to their immediate need for current or pending operations, with the intent of delivering the capability as soon as feasible to meet operational requirements. Operational requirements documents take these need statements and provide a more detailed level of operational and performance requirements, identifying the threshold and objective requirements for the desired capability.

Mr. John Clemens, a defense contractor assigned to the Air Force's functional management office for cyberspace operations, noted that a "well-defined requirement is the true source of stagnation" in fielding viable cyberspace capabilities, and that "requirements definition is the make-or-break part" in focusing effort to satisfy the operational need.[19] As is the case with other defense programs, requirements are developed with an eye towards broad application against a number of potential adversaries. This is done for perceived cost savings in having one system capable of satisfying a number of operational requirements. In an effort to achieve operational capability on a broader scale, more immediate and refined operational needs are left unsatisfied until they can be consolidated and integrated into other network warfare development efforts.

[19] John Clemens (Northrop Grumman Corporation), interview with the author, 25 February 2009.

This leaves network warfare leaders and operators frustrated as they wait for an incremental capability delivery. "Just give me anything," says Colonel Shwedo.[20]

Operational requirements documents are not typically focused on a single adversary; that is, materiel capabilities are not tailored for a single adversary or a single combat environment. Conventional military forces do not focus on one contingency, nor are their materiel capabilities intended to satisfy operational requirements in only one region or type of conflict. Cyberspace operations, however, are required to do just that. An operational requirement to affect a certain type of network may exist in multiple regions, but the application which achieves the desired effect may be so tailored to a single adversary network and its system components that it does not have utility against any other network, perhaps even in the same country or region.

Similarities exist in satisfying other non-conventional military force needs. Speaking of irregular warfare and stability operations, Secretary of Defense Robert Gates commented that "conventional modernization programs seek a 99 percent solution over a period of years," while more immediate needs in irregular warfare operations might be achieved with a 75 percent solution within a few months.[21] The analogy applies to the cyberspace domain as well. The Pareto Principle and its unintended consequences come to mind. The 80 percent solution might be achieved in 20 percent of the allotted development time, while the remaining 20 percent of requirements account for the remaining 80 percent of the delivery schedule. A requirement process focusing more on specific capabilities and adversary networks would be more effective in fielding operationally-relevant, cyberspace capabilities.

Delivery time is an exceptionally valued commodity for network warfare operators. Typically, we associate delays in capability delivery with a failure of the acquisition community

[20] Col Bradford Shwedeo (67th Network Warfare Wing), interview by the author, 25 February 2009.
[21] Robert Gates, "Preparing the Pentagon for a New Age," Foreign Affairs, January and February 2009.

to produce the required item. Before the acquisition community can begin its efforts, however, it must have an identified and vetted requirement. In this regard, the mission area managers and lead requirements organizations play an essential step in shepherding the requirement through the staffing approval process. For the leadership and operators in the network warfare community, that watch towards the clock begins when their operational deficiency or mission requirement is identified to the staffing elements.[22]

The timelines associated with macro-level documents such as the network warfare community's mission area plan approximate a year in development and coordination. Additionally, their publication is timed so that it purposefully leads into the next planning, programming and budgeting process, with the intent to gaining advocacy for future funding. This process may work well for traditional military systems that are developed over years and have operational capability throughout their warfighting domain, but it does not promote timely identification or investment towards priority efforts in network warfare operations. Planning documents which are produced one or two years in advance of the capability being developed do not offer sufficient direction in focus. Further, requirements development and then later coordination through the resource allocation process could equate to two or three years delay before research work is applied towards solving the operational deficiency.

When considering the "web year" pace at which technology may change in a targeted network and wide range of components that may be affected, time between identified need and capability delivery must be compressed. Capt Eric Stride, cyber operations action officer within the 67th Network Warfare Wing, comments that, "effective computer network attack requires multiple tools and capabilities used in concert. The target set and battlespace are quite dynamic

[22] Jeffrey Faucheux (Harris Corporation), interview with the author, 2 February 2009.

and the needs to keep up with changes in those entities are critical to success."[23] If the process, he says, "prevents timely delivery of capabilities due to inefficiencies, then that will directly impact the mission effectiveness of network warfare forces."[24] The requirements generation process must be shortened so that the acquisitions community can focus its efforts on the most urgent needs. Lt Col Fred Baier, program element monitor for network warfare systems, agrees that more attention must be put towards the requirements generation process to ensure limited resources are allocated to the most worthwhile and best defined efforts.[25]

Dr. William Perry, former Secretary of Defense, relayed his frustration with the requirements process in his efforts to develop advanced technology programs while serving as the Undersecretary of Defense for Research and Engineering in the late 1970s. He noted that to push requirements through the defense bureaucracy, there had to be constituency supporting the program. If that senior level advocate did not exist, then the program typically was not supported within a military service. Dr. Perry made this comment with respect to his efforts in establishing programs for stealth aircraft, advanced intelligence sensors and precision guided munitions. These were the "right choices with thoughtful uses, and bought smarter" than other military procurement programs of their day. Yet, Dr. Perry still met resistance from individual military services in pursuing these promising technologies. Their requirements processes had not generated these concepts as solutions to their operational needs and they sought other investments until they were obligated down the path towards more advanced capabilities.[26]

Current processes do not appear to support an abbreviated requirements generation process. Operational requirements documents are written, staffed and approved over such a long

[23] Capt Eric Stride (67th Network Warfare Wing), interview with the author, 13 March 2009.
[24] Ibid.
[25] Lt Col Fred Baier (Office of the Secretary of the Air Force), interview with the author, 12 February 2009.
[26] Dr. William Perry (former Secretary of Defense), interview with the author, 2 March 2009.

timeframe that the operational need may be obsolete before the capability is delivered or even more pressing operational deficiencies may be identified. As General Cartwright commented, "it takes longer to declare a new (program) start than the lifecycle of the software package" in the information technology arena. Technology intensive systems conducting network warfare would find this to be true in their materiel development as well.[27]

Resource Allocation

It's often said in the Pentagon that a vision or requirement without funding is known as a hallucination. The attempt at humor is sometimes lost on those that have not worked there, but it is an accurate representation of how the Department of Defense works. There may be any number of validated requirements. If funding has not been established, however, an actual program does not exist and development efforts are not permitted. This underlies the importance of the resource allocation aspect of capability development. Should an operational need be identified by network warfare operators and successfully staffed through their organizational chains, it cannot be assumed that the requirement will be funded. Perhaps even worse, a requirement might work its way through the resource allocation process and obtain funding, but on a timeline which does not allow rapid capability development.

There are different funding cycles for defense spending. In Pentagon terminology, there are the "out years" associated with future year spending and the Service's Program Objective Memorandum, the "budget year" which identifies the next fiscal year's spending plan, and the "execution year" which defines expenditures within the current fiscal year. Elements within each of these funding processes are occurring in some form at the Pentagon each day, although there are particular periods on the calendar in which one may rise in visibility and importance. Of

[27] Antonie Boessenkool, "DoD IT Procurement Too Slow: Cartwright," Defense News, 4 March 2009.

more importance are the time horizons these funding processes have, the staffing duration allocated to each and the impact on network warfare operators.

The Program Objective Memorandum is arguably the most important of these funding processes. It establishes programs of record and future funding to either satisfy a new requirement or sustain an existing mission capability. As applied to a network warfare system, the requirement would be endorsed by the cyberspace operators' major command and submitted to the Air Force corporate process for funding consideration. Let us assume that such a requirement is funded. This resource approval does not result in the immediate expenditure of dollars towards the cyberspace operators' requirement. Instead, it results in a resource funding wedge at least two years in the future. Given the nature of emerging targets, network innovation and changing technology, it's difficult to identify needed operational requirements in the cyberspace domain within the next six months. Mr. Brown, deputy director for intelligence and requirements at Air Force Materiel Command, concurs: "the (Program Objective Memorandum) cycle is too long."[28]

As noted previously, one intent behind the planning, programming and budgeting process is to provide "output oriented, well documented, (and) systematically accountable" process. The Department of Defense and the Service wants to ensure a structured and reproducible flow of like information to the resource allocation process. This ensures priorities are identified, costs are assessed and resources allocated to the more worthwhile efforts. Because it is to be a well documented process, requirements considered for funding consideration provide similar types of information. One of those items to be considered is technological risk and the maturity of the enabling technology. Just as it is difficult to anticipate what technologies and applications might be faced in the cyberspace domain either 12 or 24 months in the future, it is also difficult to

[28] Randy Brown (Air Force Materiel Command), interview with the author, 2 February 2009.

identify what methods our cyberspace operators and developers may take in affecting those future networks. This unknown level of threat and how it will be addressed could work against a network warfare development effort being recognized as mature and worthy of funding.

On more near-term timeframes, the Service budget is being developed and execution year dollars are supporting current cyberspace development efforts and operations. These funding processes begin with amounts identified in earlier Program Objective Memorandum efforts. With the more difficult task of getting out year funding secured, it would seem that budget and execution year processes would pose little difficulties. Unfortunately, that is not the case.

Programs are funded to a top-line level. That is to say that there is a finite bound on the overall program expenditures. Within that top-line, funding is specified for operations, development, procurement and other purposes. This nuance and how those dollars are overseen further complicate the resource allocation and funding distribution process for network warfare operations. Ultimately, it affects the cyberspace community's ability to move funding to pop-up targets, emerging opportunities or new technologies.

In the defense community, these funding lines are known as "colors of money." For example, funds provided for operations and maintenance comprise a type of appropriation code known as "3400." Research, development and acquisition efforts are funded with the "3600" appropriation code. These mechanisms are established to not only provide accountability to see where defense dollars are being spent, but also to provide a means to legally ensure they are being expended as directed by Congress. Funded network warfare programs are managed just as other mission areas and their programs are also funded by these different "colors of money."

Difficulty arises, however, when one wishes to convert one appropriation type to another. For example, let's consider a network warfare program that has been funded at a level of $10 million in the current budget year. Half of that might committed towards operations and maintenance costs (appropriation 3400), while the remaining $5 million might be budgeted towards research, development and acquisition efforts (appropriation 3600). Now consider a scenario where one needs to invest additional monies against a pop-up target or to leverage a new technology to satisfy an operational need.

The functional managers within the network warfare community simply cannot take unused operations and maintenance monies and allocate them towards the new development effort, nor do they have the authority to take existing development dollars and apply them towards the potentially lucrative development efforts. Legally, the program managers are obligated to spend those dollars as they have been appropriated to them until they have approval from the corporate process to move those dollars to new efforts.

The need to quickly re-direct development efforts is an operational necessity within the network warfare community, but not necessarily one within the development efforts of other warfighting domains. Technological opportunities may arise in other conventional weapons development programs, but they do not occur with the frequency and rapidity as they may in the cyberspace domain. For those outside the network warfare community, identifying a new development area and attempting to re-allocate resources may suggest a program that is assuming risk and not technologically mature. Network warfare operators, however, see this as an essential method to leverage "best of breed" and emerging technology that may not have been available when the initial development solution was identified.

There does appear to be some recognition of this problem and steps are being taken to address this issue within the functional management offices overseeing resource investments for cyberspace operations and development. Lt Col Baier, tasked with program oversight for cyberspace research and acquisition efforts, commented that he has gained flexibility in moving investment dollars around within his portfolio. This resource "maneuver room," as he calls it, is essential in making sure what limited dollars the community has available is put towards those most pressing needs and promising technologies.[29]

Development and Acquisition

After the requirements and resource allocation processes are completed, the development and acquisition process can begin. It faces its challenges as well in fielding effective cyberspace capabilities, just as other weapons systems development efforts experience in other warfighting domains. Satisfactory cost, schedule and performance are not necessarily assumed to result in this process, as shown previously in the findings of the Government Accountability Office. Unfortunately, delivery and system capability shortfalls have more immediate effects on network warfare operations.

The acquisitions processes within the Department of Defense have been critiqued frequently over the past decades, with many finding fault in their seeming inability to deliver promised systems on a timeline acceptable to the end user, while also remaining within budget limitations. There have been numerous "blue ribbon" commissions established to review these acquisition processes, yet all of these have been focused on acquisition guidelines, directives and procedures for traditional weapons systems development and procurement. There has not yet been a study focused on how network warfare systems are ill-served by a process that becomes more rigid with each study.

Lt Col Tamara Schwartz, chief of the cyberspace capabilities integration office within Air Force Materiel Command, commented that new revisions in the Department of Defense's

[29] Lt Col Fred Baier (Office of the Secretary of the Air Force), interview with the author, 12 February 2009.

primary acquisitions directive "actually makes the process more onerous" for cyberspace capability development.[30] According to Mr. John Young, Under Secretary of Defense for Acquisitions, the objectives of the new "5000-series" acquisition directive were "controlling cost and helping the Services deliver products on time."[31] This was to be achieved through "more frequent and effective program reviews to assess progress," as well as assessments of their technology readiness. Additionally, "changes call for beefed-up testing" of development efforts.[32]

This is but one example of how what might be good for traditional weapons system development is detrimental for network warfare efforts. Col Shwedo, commander of the 67th Network Warfare Squadron, noted that the culture of the testing community must be changed with respect to cyberspace capabilities.[33] Traditionally, operational test and evaluation personnel are committed to testing every performance capability to their 100% satisfaction. This is understandable, as it is their certification and approval which warrants future government acceptance of the capability. However, Colonel Shwedo commented that the test and evaluation community are not sufficiently focused on the sense of urgency in bringing a capability "online." Instead he believes a new manner of testing should be established which allows a confidence factor of the testers, which is then accepted or rejected by the operational commander as a consideration of risk.[34]

Mr. Robert Giesler, vice president for cyber programs for a major defense contractor, concurred with the difficulties associated with the testing process. He believes the approach taken towards computer network weapons is due to the excessive promotion of potential

[30] Lt Col Tamara Schwartz (Air Force Materiel Command), interview with the author, 6 March 2009.
[31] John Bennett, "New US Acquisition Policy Approved," Defense News, 3 December 2008.
[32] Ibid.
[33] Col Bradford Shwedo (67th Network Warfare Wing), interview with the author, 25 February 2009.
[34] Ibid.

capabilities in their early development days. Some in the cyberspace community suggested "mass destruction-like effects," such as shutting down a country's entire electronic grid or destroying its telecommunications network. Such statements led some to view cyberspace operations as having the same "nationwide effects" potential as nuclear weapons, which then led to "two-key launch" mentalities and the thought that Presidential or Secretary of Defense-level authorization was needed. "We are a victim of our own hyperbole," with respect to network warfare effects and it's "resulted in a governance structure" such as that befitting more potent systems.[35]

Other frustrations besides testing were noted by leaders and subject matter experts within the community. One common theme was the inability to integrate new technology as it was made available to the commercial sector. Dr. Perry commented that even during his days as Secretary of Defense that many technology efforts developed outside of defense programs were far more advanced than similar efforts inside the department. In some cases, he found that military programs had been surpassed by what was commercially available and that the military systems were "two generations behind in terms of effectiveness."[36]

This reluctance to adopt new technology, particularly one that is software intensive, was also mentioned by Mr. Giesler. In his experience when dealing with government acquisition officials, the focus appears to be on the platform and hardware solutions.[37] His thoughts were echoed by Lt Col Douglass Coppinger, commander of the 91st Network Warfare Squadron. Describing his relationship with the acquisitions offices responsible for satisfying his operational needs, he cites a mindset which "defaults towards a hardware solution."[38] The effect in not

[35] Robert Giesler (SAIC), interview with the author, 19 February 2009.
[36] Dr. William Perry (former Secretary of Defense), interview with the author, 2 March 2009.
[37] Robert Giesler (SAIC), interview with the author, 19 February 2009.
[38] Lt Col Doug Coppinger (91st Network Warfare Squadron), interview with the author, 26 February 2009.

adding promising software solutions is not only to lengthen the timeline for delivery, but also the production of a less-than-capable system. "There is a disconnect between what is said (as a requirement) and what is delivered (in acquisitions)," said Lt Col Coppinger.[39]

Operators also noted the time delay between requirements identification to an acquisition effort being initiated. As mentioned earlier regarding the requirements generation and resource allocation processes, the acquisitions community is somewhat dependent on a well-defined requirement and sufficient resource investments being approved before they can begin their own effort. Still, delays can and do occur in initiating the acquisitions process even with those staffing obstacles surmounted.

Lt Col James Lance, deputy commander of the Air Force's Network Operations Center, commented that the bureaucracy sometimes overwhelms even the best intentions to provide even rudimentary capabilities to cyberspace operators. After submitting concept of operations and operational requirements documents for a network defense system in October 2007, it still had not been released as a "Request for Proposal" to industry within the following 18 months.[40] He also mentioned that his organization's "defense industry partners had developed several promising prototype systems" to satisfy the requirement, but that they were unable to purchase or develop the systems further without a break in the bureaucratic staffing. From his perspective, Lt Col Lance sees this as "but one example of an inflexible Cold War-era acquisition system not optimized for the 21st century Air Force" or the cyberspace domain.[41]

[39] Lt Col Doug Coppinger (91st Network Warfare Squadron), interview with the author, 26 February 2009.
[40] Lt Col James Lance (Air Force Network Operations Support Center), interview with the author, 27 February 2009.
[41] Ibid.

Chapter 4

Potential Alternatives for Success

> *We must be prepared to change requirements and operating procedures to agree with commercial practice if we are to make efficient use of commercial technology.*
>
> — United States Air Force Scientific Advisory Board

In discussions with current and former senior leaders, several suggestions were made as to how policies and processes might be altered to address these challenges. There was broad agreement across the small sampling of subject matter experts to which I spoke that there must be some considerations and allowances made for the unique operational environment in which cyberspace operations occur and the enabling technologies which lead to operational success. Without modifications, it was commonly stated that our network warfare capabilities will not be as robust, capable or effective as needed in a demanding cyberspace environment.

Three alternatives are identified here which will address the challenges facing cyberspace materiel development. Together, these alternatives provide a tiered approach to countering some ill effects of the corporate processes, while also mitigating both operational and resource allocation risk. Additionally, it allows for a more responsive presentation of materiel development capabilities to counter the unique challenges of technology breadth, pace of innovation and operational urgency.

Major Force Program-11 Authorities

The United States Special Operations Command (USSOCOM) has unique procurement authorities provided to it by law. It is the only joint combatant command which is provided its own procurement funding to purchase equipment for its component forces, independent of that component's parent Service. In all other joint combatant commands, parent Services are identified in federal statute as being responsible for satisfying all materiel and equipment needs of their respective forces.

USSOCOM's special authority is known as Major Force Program-11 (MFP-11). This authority was granted by the United States Congress, upon recommendation of the Secretary of Defense and an appointed commission, following inquiries into the failed 1979 rescue attempt of the Americans held hostage by Iranian revolutionaries. This review assessed the underlying causes of the mission's failure. In part, the commission found that equipment and interoperability issues contributed to other unanticipated issues which ultimately prevented completion of a successful mission. Additionally, it was determined that a joint combatant command was required to coordinate not only operational components, but to satisfy the specialized procurement needs of those forces.

Given the nature of special operations, their unique operational environments, and the potential for immediate force employment, it was determined that the to-be-established USSOCOM required unique procurement authorities. MFP-11 allows USSOCOM to acquire unique equipment for its forces and operations, with more tailored operational requirements than what might occur had their needs had been filled by traditional procurement processes within the Services. It also allows USSOCOM to approach and directly work with potential industry partners to develop technologies and military components that might satisfy existing operational needs or future operational concepts.

A similar procurement authority for a joint cyberspace component would also be appropriate.[42] With this, the joint command could identify its own unique requirements and then work within an abbreviated and more tailored process which specifically focuses on network warfare. Additionally, industry partners and innovators would have a more identifiable entry into a joint organization capable of not only identifying the requirements, but also procuring them. This authority would also promote a more collaborative environment between the private sector and the cyberspace operations community, similar to that relationship enjoyed by the special operations community and its private sector partners.

MFP-11 authorities for a joint cyberspace command would directly address the unique challenges facing computer network operations. The breadth of technological innovation and its potential impacts on cyberspace operations would be partly mitigated by the change in process. In working more directly with the private sector and empowered with its special procurement authorities, the joint command could better anticipate the deployment of new technologies which might affect targeted or intended target components. This may not prevent technological surprise on all adversary networks; however, the improved awareness may lessen the time needed to orient to the problem and enable a more refined course of action to be developed more quickly when those situations develop.

Additionally, MFP-11 might help the joint command better respond to the pace of technological innovation and how it affects their target networks. Similar to its ability to lessen orientation time to the problem as noted above, it would provide a more proactive means to correct deficiencies resulting from the rapid employment of a new technology or application.

[42] Robert Giesler (SAIC), interview with the author, 19 February 2009.

Special procurement authorities would allow a more immediate response from a cyber-focused command than would a similar response that required a more lengthy approval process through the Service's headquarters element. The community would not only have the core expertise to recognize the operational problem, but it would also have the resource means to invest in a solution in a much more timely manner.

The final challenge was that of operational urgency, largely resulting from frequent requests of operational leaders and forces encountering unforeseen threats or opportunities in the current operating environment. MFP-11 would also be a helpful tool in addressing this challenge by reducing the time from recognition of the problem to resources being applied to the problem. With these special authorities would come the ability to reprogram monies from a lesser priority to a higher priority, such as those identified by an operational commander. MFP-11 would allow the joint forces commander responsible for cyberspace forces to redistribute resources within the command as the operational environment changes. This not only provides a more responsive command to these operational urgencies, but also encourages a continual reassessment of materiel development programs and their relative priority and potential impact on operational capability.

A key challenge in establishing these authorities is the creation of a joint forces command for cyberspace operations. Currently, Air Force network warfare capabilities are presented through the Joint Force Component Commander for Network Warfare, an organizational element of the United States Strategic Command (USSTRATCOM). While it may be possible to assign specified procurement authorities to USSTRATCOM for the cyberspace mission, this approach is without precedent. There are recent news reports of the Secretary of Defense considering a joint combatant command for network warfare and this would be a critical first step towards establishing future MFP-11 authorities.

CYBER SAFARI

Another successful approach which might be leveraged by the cyberspace community is that of BIG SAFARI.[43] This is a quick reaction capability organization focused on providing tailored equipment and capabilities to Air Force intelligence platforms. BIG SAFARI is an Air Force Materiel Command unit, located within the Aeronautical Systems Center at Wright-Patterson Air Force Base. Its aim is to rapidly develop new sensors and systems associated with airborne intelligence platforms. It does this on a platform-centric basis, focusing on incremental improvements to a single aircraft and then making those same modifications throughout the airborne fleet at some point in the future.

This program has had broad and sustained success for several decades, enabling improvements to intelligence gathering systems to become operational at a quicker pace. This is due to its ability to focus effort towards emerging threats within the changing operational environment, as well as the manner in which their deliverable products are quickly pushed out to an airborne platform and then the remainder of the fleet. The fleet is modified on an incremental "as can occur" schedule, as opposed to a delivery schedule which requires all aircraft be modified within the same timeframe. Configuration management of the airborne fleet is a challenge; however, the overall operational capability of the fleet improves incrementally over time.

As applied to network warfare, CYBER SAFARI could be a similar organization. Given the nature of cyberspace operations and the need for close, timely exchanges between operators and

[43] Randy Brown (Air Force Materiel Command), interview with the author, 2 February 2009.

the materiel developers, the organization would best be collocated with the operational cyberspace organizations. It then could focus on satisfying the emerging operational needs with a similar quick reaction capability as is displayed by BIG SAFARI.

CYBER SAFARI would be an excellent option in countering the effects of both broad and narrowly-focused technological changes to targeted networks. The organization would not be responsible for developing capabilities against new networks, but rather making modifications to friendly capabilities to ensure operational advantage is maintained or regained. For example, an existing offensive capability targeting a specific adversary network may experience a situation where a single component or series of components within that network negates or reduces the platform's ability to successfully engage it. CYBER SAFARI, following notification and direction by the operational community, would focus effort towards a solution which enables that offensive capability to regain access and network maneuverability.

This organization would also be helpful in addressing the pace of technological innovation on the targeted networks. Adversaries will integrate new technologies, applications and bundled services into their networks at different speeds. Some may consistently be more aggressive in modifying their network, while others may frequently lag others in making modifications. More likely is that an adversary will range across the spectrum. CYBER SAFARI would allow quick reaction efforts that were focused on one network to be more broadly applied against other targets before changes in those secondary networks were ever observed. With the organization focused on providing solutions to identified deficiencies in existing capabilities, CYBER SAFARI will likely be working towards solutions that could then be exported to other platforms targeting other networks. This would allow those other platforms to be incrementally improved, just as the airborne intelligence fleet.

Clearly, the CYBER SAFARI concept would be responsive to the third challenge of operational urgency, particularly if the organization were located in close proximity to the cyberspace operators. Although the organization may not have physical presence near all network warfare platforms or their forces, the concept would enable a more timely dialogue between the operations community and the materiel capability developers. Additionally, the organization would allow a more focused support effort to the existing and employed capabilities. CYBER SAFARI, like its BIG SAFARI model, would be a critical improvement towards quick reaction capability development.

Cyber Warfare Integrated Reprogramming

An adaptation of the Electronic Warfare Integrated Reprogramming (EWIR) effort would also provide improvements to cyberspace systems.[44] EWIR is a program focused on providing sensor, intelligence and other adjustments to fielded electronic warfare systems. These systems are not aircraft themselves, but primarily radar warning receivers and electronic jammers throughout the air operations community. Using intelligence data, collected signals, data simulation models and other techniques, EWIR identifies new threats and then pushes updates to the affected receivers and jammers.

For example, consider the instance where an intelligence platform identifies a new radar signal associated with a surface-to-air missile and that the presence of this signal is associated with the terminal guidance radar for the missile. The EWIR program office would take this previously unknown signal and then identify the unique parametric data associated with it. After modeling the signal's characteristics and understanding its role in the adversary surface-to-air missile system, the EWIR office would publish an electronic notice of the new signal to the air

[44] Mike Mintor (MITRE), interview with the author, 2 March 2009.

operations community. Specialists there would take that information and reprogram their respective organizations' radar warning receivers and jammers, allowing their aircraft to now have an awareness of this new signal and its importance. In this way, the aircraft are now able to sense the threat and electronic warfare aircraft are now able to jam the associated radar more effectively.

A similar model could be used for cyberspace operations. A Cyber Warfare Integrated Reprogramming (CWIR) office would perform a similar purpose in collecting network-associated information, modeling that data to understand its operational impact, and then push out capability impact reports to the cyberspace forces. For example, suppose intelligence sources indicated a specific technology change was to take place on a targeted adversary network. The CWIR office could acquire a commercial copy of the component to be changed or the technical specifications of that upgrade, and then perform its own assessment of how the change may affect our known operational capability. The CWIR office might make use of a test facility with a variety of different representative networks on which they could replicate modifications to determine their impact. The office might then provide software updates to fielded capabilities so that those systems were prepared for the pending upgrade on the targeted network. Operational units could also review CWIR reports to determine whether additional adjustments where needed in their tactics.

A CWIR model would provide an organization that was focused on detecting technology changes in targeted networks and then developing some initial response for the community to counter it. This addresses the need for cyberspace materiel development processes to be cognizant and responsive to the breadth of potential change on adversary systems. The CWIR organization, working with operator and intelligence community information, would be able to compile a central repository of these changes as they are applied in networks around the world. This would allow capability developers and cyberspace operators advance warning of potential changes and remedies to other problems.

The pace of technological change might also be captured and tracked by the CWIR organization. Using its collected intelligence information and network modeling tools, it may be able to develop forecasting methods to understand how quickly changes may propagate through a representative network using the same types of upgrades or how likely another network is to employ similar changes. The most valuable use of CWIR might be in providing a deeper technical understanding of how targeted networks are changing over time and whether there are certain networks that are more agile or likely to change.

CWIR is perhaps the most responsive towards satisfying the operational urgency challenge. If following the EWIR model, this organization would actually identify potential issues and operational shortfalls before the operators themselves might be aware. In the earlier example of the new threat radar system, a single indication of a new signal would be a threshold event requiring an update to be pushed to all radar warning receivers and electronic warfare jammers. CWIR, if using a like example, would detect a single change on a targeted adversary network and push a potential fix to affected operators. This would be a very proactive means to support the operational community.

There are challenges in applying the EWIR model to the cyberspace domain, one of which would be in determining the scope of responsibility of the CWIR organization. Some solutions may be worked in-house with available skills sets and resources; however, others might require significantly more effort or expertise which is not resident within it. This may require some triage function internal to CWIR which sorts deficiencies to those that can be resolved within the organization and those which require outsourcing.[45]

[45] Mike Mintor (MITRE), interview with the author, 2 March 2009.

Chapter 5

Conclusion

> *Information warfare will be the most complex type of warfare in the 21st century, and it will decide who will win and who will lose the war.*
>
> — Chang Mengxiong, Chinese military theorist

The Department of Defense and the Air Force are still developing their organizational structures and operational concepts for network warfare. And they both are beginning to place more attention on the forces and training required for this newest warfighting domain. Concurrently, they are developing and fielding materiel capabilities for future cyberspace operations, directed both against potential adversaries and ensuring the security of our own networks. As the network warfare mission area matures and data points are gathered on how those capabilities perform, it is likely that some will identify problems in the corporate processes to deliver those needed platforms and tools.

The corporate processes used by the Department of Defense and the Air Force were developed in a different era of military capability production. These are industrial-era bureaucratic processes which are geared towards the production of traditional military systems and equipment, particularly those made in large quantity. The processes do have advantages in identifying highest priority needs, allocating limited resources to those priority needs and then ensuring appropriate oversight to the acquisition of those capabilities. However, the operational environment of cyberspace is much different than the warfighting domains of air, space, ground and maritime operations. This uniqueness in operations minimizes the benefits of the process, while amplifying the negative aspects of the bureaucracy.

Network warfare capabilities are much more vulnerable to technological surprise. Friendly networks which were secure one day may be vulnerable tomorrow. Similarly, adversary networks which could be effectively targeted in one configuration might regain their security in short duration due to a slight modification. The only way in which our cyberspace operations capabilities maintain or gain advantage is to ensure that our platforms can be modified quickly to address these changes.

The cyberspace domain is defined by the technology being employed. How that technology is employed, whether in hardware or software elements, and our ability to either protect or exploit the desired networks will depend on our ability to stay apace with the changes. Breadth and pace of technological innovation will be a critical stressor on our materiel development capabilities, with our operators adding to this by identifying new threats or deficiencies. Whatever methods are used must consider these aspects.

Offered within this paper are three alternatives to these challenges: special procurement authorities, a quick reaction capability organization, and another organization to focus on network environmental updates. Respectively, these were Major Force Program 11 authorities, CYBER SAFARI and the Cyber Warfare Integrated Reprogramming effort. Ideally, these three alternatives would be implemented as a package, enabling unique effects at different levels in the development, acquisition and procurement of materiel capabilities. It is my recommendation that all three alternatives be adopted.

Bibliography

Air Force Cyber Command, "New Cyberspace Career Fields, Training Paths, Badge Proposed," http://www.afcyber.af.mil/news/story.asp?id=123104963 (accessed 15 Dec 2008).

Air Force Doctrine Center. *Air Force Doctrine Document 2-5: Information Operations*. Maxwell AFB, AL: Air Force Publications, 11 January 2005.

Air Force Link, "Air Force Releases New Mission Statement," http://www.af.mil/news/story.asp?id=123013440 (accessed 10 December 2008).

John Bennett, "New US Acquisition Policy Approved," Defense News, 3 December 2008.

Antonie Boessenkool, "DoD IT Procurement Too Slow: Cartwright," Defense News, 4 March 2009.

Carol L. DeCandido, *An Evolution of Department of Defense Planning, Programming and Budgeting System: From SECDEF McNamara to VCJCS Owens*, US Army War College Strategy Research Project (US Army War College, Carlisle Barracks, PA, 4 June 1996).

Robert Gates, "Preparing the Pentagon for a New Age," Foreign Affairs, January and February 2009.

Rebecca Grant, "The Cyber Menace," Air Force Magazine, March 2009.

Headquarters United States Air Force Program Action Directive 07-08, "Phase I of the Implementation of the Secretary of the Air Force Direction to Organize Air Force Cyberspace Forces," 20 February 2009.

HQ USAF/XP, "Global Engagement: A Vision for the 21st Century," http://www.au.af.mil/au/awc/awcgate/global/competencies/information.htm (accessed 15 January 2009).

Joint Staff. *Joint Publication 3-13: Information Operations.* Washington D.C.: Joint Publication, 13 February 2006.

Tamara B. Schwartz, "Capabilities Without Borders," Electronic Security Center (Boston, MA, undated).

US Government Accountability Office, *Best Practices: Stronger Practices Needed to Improve DoD Technology Transition Process*, Report to Congressional Committees, GAO-06-883 (Washington DC, September 2006).

US Government Accountability Office, *Defense Acquisitions: Results of Annual Assessment of DoD Weapon Programs*, Testimony to the House of Representatives, GAO-08-674T (Washington DC, 29 April 2008).

US Government Accountability Office, *Defense Acquisitions: DoD's Requirements Determination Process Has Not Been Effective in Prioritizing Joint Capabilities*, Report to the US Senate, GAO-08-1060 (Washington DC, September 2008).

US Government Accountability Office, *Defense Acquisitions: Fundamental Changes are Needed to Improve Weapon Program Outcomes*, Testimony before the US Senate, GAO-08-1159T (Washington DC, 25 September 2008).